

REMARKS

The Office Action dated February 28, 2007, has been received and carefully noted. The following remarks are submitted as a full and complete response thereto.

Claims 1-2 and 4-21 are currently pending in the application, of which claims 1, 10, and 19-21 are independent claims. Claims 1-2 and 4-21 are respectfully submitted for consideration.

Claims 1-5, 10-13, and 19-21 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,887,251 of Fehnel (“Fehnel”) in view of U.S. Patent No. 6,678,281 of Chakrabarti (“Chakrabarti”) and “Global Authentication” of Marcovici et al. (“Marcovici”). With regard to independent claims 1, 10, and 19-21, the Office Action took the position that Fehnel teaches many of the features of the claims, but cited Chakrabarti to remedy one deficiency (with respect to “a GPRS network involved in authentication”) and Marcovici to remedy other deficiencies (“authenticating the network to the mobile node” and “wherein the authentication the mobile node is performed in a single round trip while the mobile node is roaming”). Applicants respectfully traverse this rejection.

Claim 1, upon which claims 2 and 4-9 depend, is directed to a method including sending a random number to a mobile node, wherein the random number is generated local to the mobile node, wherein the random number is generated by a base station. The method also includes generating a mobile node signature using the mobile node, wherein the mobile node signature is generated using the random number. The method further

includes authenticating the mobile node to a network, wherein the network is a general packet radio service network. The method additionally includes authenticating the network to the mobile node. The authenticating the mobile node to the network and the authenticating the network to the mobile node is performed in a single round trip while the mobile node is roaming.

Claim 10, upon which claims 11-18 depend, is directed to a system including a mobile node that is configured to generate a mobile node signature in response to a random number received from a source within a domain local to a current position relating to the mobile node and send the mobile node signature to be verified, wherein the random number is generated by a base station. The system also includes the authentication server located within a home domain associated with the mobile node that is configured to receive the mobile node signature, verify the mobile node signature, and in response to the verification of the mobile node signature that indicates that the mobile node is verified to a network, wherein the network is a general packet radio service network, return an authentication signature to the mobile node. The verification of the mobile node by the authentication server and verification of the authentication signature by the mobile node is performed in a single round trip while the mobile node is roaming.

Claim 19 is directed to a system including a base station for generating a random number local to the mobile node. The system also includes a means for sending the random number to the mobile node. The system further includes a means for generating a mobile node signature using the mobile node, wherein the mobile node signature is

generated using the random number. The system additionally includes a means for sending the mobile node signature to an authentication server within a general packet radio service network, and verifying by the authentication the mobile node signature; and in response to the verifying, generating an authentication signature and sending the authentication signature to the mobile node for verification. The verification of the mobile node by the authentication server and verification of the authentication signature by the mobile node is performed in a single round trip while the mobile node is roaming.

Claim 20 is directed to a base station including a random number generation unit configured to generate a random number. The base station also includes a transmission unit configured to send the random number to a mobile node that is roaming and is connected to the base station. The base station further includes a reception unit configured to receive a mobile node signature generated by the mobile node using the random number. The base station additionally includes an authentication unit configured to authenticate the mobile node to a network by communicating with an authentication server, wherein the network is a general packet radio service network. The base station also includes a provision unit configured to provide an authentication signature to the mobile node. The authenticating the mobile node to the network and the providing the authentication signature to the mobile node is performed in a single round trip.

Claim 21 is directed to a base station including random number generation means for generating a random number. The base station also includes transmission means for sending the random number to a mobile node that is roaming and is connected to the base

station. The base station further includes reception means for receiving a mobile node signature generated by the mobile node using the random number. The base station additionally includes authentication means for authenticating the mobile node to a network by communicating with an authentication server, wherein the network is a general packet radio service network. The base station also includes provision means for providing an authentication signature to the mobile node. The authenticating the mobile node to the network and the providing the authentication signature to the mobile node is performed in a single round trip.

Certain embodiments of the present invention advantageously provide single round trip authentication of a roaming mobile node using a random number generated by a base station of a foreign network (*i.e.* not the network of the mobile node). The combination of cited references (Fehnel in view of Chakrabarti and Marcovici) fails to disclose or suggest all of the elements of any of the presently pending claims, and, thus, fails to provide these critical and non-obvious advantages.

Fehnel generally relates to authentication key management for mobile stations. As explained at column 9, lines 1-39 thereof, Fehnel aims to provide an A-key management procedure that integrates existing approaches, while simultaneously avoiding maintaining lists of random A-keys for the mobile stations from each manufacturer. If a random A-key is desired, the mobile station can generate this value, or the value can be precomputed by the manufacturer.

In the background section of Fehnel, in the subsection entitled “Related Prior Art Systems,” at column 7, lines 40-62, Fehnel discusses a process of authentication. In this process of authentication the base station generates and sends to a mobile station a random bit pattern (RAND or RANDU). Each of the mobile station and the base station uses RAND or RANDU along with other parameters as inputs to an authentication algorithm known as CAVE. Based on the inputs, the mobile station or base station generates an authentication response AUTHR or AUTHU respectively depending on whether RAND or RANDU is used.

As Fehnel explains in the “Related Prior Art Systems” sub-section at column 6, lines 54-62, the authentication response computed in the mobile station is sent to the base station to be compared with the authentication response computed in the base station. If the authentication responses match, authentication is considered successful. If the comparison at the base station fails, the base station can deny service to the mobile station or update its own shared secret data (SSD).

Claim 1, for example, recites “wherein the authenticating the mobile node to the network and the authenticating the network to the mobile node is performed in a single round trip while the mobile node is roaming.” This feature is neither disclosed nor suggested in Fehnel. The Office Action recognized that Fehnel has certain deficiencies (including this deficiency) and, therefore, cited Chakrabarti and Marcovici.

Chakrabarti generally relates to a hardware confirmation, support node, and methods for implementing general packet radio services over GSM. At column 6, lines

50-62, Chakrabarti mentions in passing that one function of an SGSN can be authentication, and Chakrabarti's abstract mentions that the general packet radio services support node (GSN) described in Chakrabarti can function as an SGSN in a global system for mobile communications (GSM) network.

Unsurprisingly, therefore, Chakrabarti also fails to disclose or suggest "wherein the authenticating the mobile node to the network and the authenticating the network to the mobile node is performed in a single round trip while the mobile node is roaming" as recited in claim 1.

The Office Action acknowledged that the combination of Fehnel and Chakrabarti fails to disclosed all of the features of claim 1, and particularly this feature of claim 1, and cited Marcovici to remedy this and other deficiencies of the combination of Fehnel and Chakrabarti.

Marcovici generally relates to two proposals for allegedly enhanced subscriber architectures, 3GPP-AKA (based on GSM MAP) and LESA (based on ANSI-41). One of Marcovici's proposals (4.1) relates to authentication and session key agreement. This proposal, however, follows a proposal (3.1) for key provisioning. Indeed, Marcovici, at page 4, section 4, indicates that the proposal in 4.1 follows the procedure described in 3.1 ("Once the SSD is established, it can be used to conduct operational procedures defined in this section.").

Marcovici describes an authentication process in Figure 4.1.1-1 that includes a single round trip from the mobile station to a home location register (via a VLR) and

back. However, only a single validation is performed in the process as described (at step (e) the “Network Signature” is authenticated by the mobile), and the mobile station is not described as providing a signature.

Thus, clear distinctions exist between Marcovici’s disclosure and what is claimed as “wherein the authenticating the mobile node to the network and the authenticating the network to the mobile node is performed in a single round trip while the mobile node is roaming” as recited in claim 1.

More particularly, Marcovici’s disclosure indicates that the procedure shown in Figure 4.1.1-1 is performed after the secondary security keys are established between the mobile station and the HLR via the VLR. Accordingly, the process described by Marcovici in Figure 4.1.1-1 is not a procedure in which both the mobile node is authenticated to the network and the network is authenticated to the mobile node.

Instead, as described by Marcovici, the round trip procedure only provides a signature from the network to the mobile and only authenticates the network to the mobile.

Accordingly, Marcovici does not remedy the above-identified deficiencies of Fehnel and Chakrabarti with respect to “wherein the authenticating the mobile node to the network and the authenticating the network to the mobile node is performed in a single round trip while the mobile node is roaming” as recited in claim 1.

Furthermore, the combination of cited references constitutes impermissible hindsight reconstruction. The Office Action asserted that it would have been obvious to

combine the teachings of the three references, citing Marcovici's assertion that Marcovici's proposal provides enhanced security at page 2, section 1, and citing Chakrabarti's assertion that GPRS provides better support for bursty data.

The cited motivation in Chakrabarti is just a generally positive statement regarding the value of GPRS, not a teaching, motivation, or suggestion to modify the authentication process described by Fehnel. Furthermore, the proposed motivation relates to data traffic, but Fehnel is directed to a system that primarily targets voice communications, as can be seen from column 1, lines 12-26. Accordingly, one of ordinary skill in the art having Fehnel's objects in mind would not be motivated to modify Fehnel's authentication process based on the disclosure of Chakrabarti, because it would not be expected to effect the objects of Fehnel's disclosure

Moreover, the proposed motivation to combine Marcovici's disclosure with that of Fehnel and/or Chakrabarti is also legally insufficient. The proposed motivation is to enhance security. In contrast, however, the teaching for which Marcovici is principally cited (*i.e.* performing the authentication in a single-round) is not a modification that one of ordinary skill in the art would expect to enhance security. Accordingly, the proposed motivation does not relate to the teaching selected from the cited reference.

Additionally, the alleged enhancement of security proposed by Marcovici would suggest, if anything, that one of ordinary skill in the art simply use Marcovici, not that one of ordinary skill in the art modify the teachings of Fehnel based on the disclosure of

Marcovici. For this additional reason, the proposed motivation to combine is legally insufficient.

Accordingly, for these additional reasons, it is respectfully requested that the rejection be withdrawn because there is no legally sufficient motivation to combine the references so as to produce what is claimed.

Independent claims 10 and 19-21 each have their own scope. Nevertheless, claims 10 and 19-21 were not separately rejected, and, thus, the distinctions presented above with respect to claim 1 also serve to show that claims 10 and 19-21 are patentable.

Claims 2-5 and 11-13 depend from, and further limit, claims 1 and 10. Thus, claims 2-5 and 11-13 each recite subject matter that is neither disclosed nor suggested in the combination of Fehnel, Chakrabarti, and Marcovici. It is, therefore, respectfully requested that the rejection of claims 2-5 and 11-13 be withdrawn.

Claims 6-9 and 14-18 were rejected under 35 U.S.C. 103(a) as being unpatentable over Fehnel in view of Chakrabarti and Marcovici and further in view of U.S. Patent No. 6,894,994 of Grob et al. ("Grob"). The Office Action took the position that the combination of Fehnel, Chakrabarti, and Marcovici fails to disclose certain further limitations of the claims. The Office Action cited Grob to remedy these deficiencies. Applicants respectfully traverse this rejection.

Claims 6-9 and 14-18 depend respectively from, and further limit, claims 1 and 10. At least some of the deficiencies of the combination of Fehnel, Chakrabarti, and Marcovici with respect to claims 1 and 10 are discussed above. Additionally, the lack of

prima facie motivation to combine Fehnel, Chakrabarti, and Marcovici is discussed above.

Grob fails to remedy the above-identified deficiencies of Fehnel, Chakrabarti, and Marcovici, and fails to provide a motivation to combine Fehnel, Chakrabarti, and Marcovici or to combine itself (Grob) with Fehnel, Chakrabarti, and Marcovici. Thus, the combination of Fehnel, Chakrabarti, Marcovici, and Grob fails to disclose or suggest all of the elements of any of the presently pending claims.

Grob generally relates to a high data rate wireless packet data communication system. Grob aims to provide a high speed wireless packet data communication system capable of providing wireless Internet services and other packet data services. Grob aims to provide a system based on a distributed architecture and which includes elements that can be easily deployed and upgraded.

Accordingly, it is unsurprising that Grob is silent as to “wherein the authenticating the mobile node to the network and the authenticating the network to the mobile node is performed in a single round trip while the mobile node is roaming” as recited in claim 1. Consequently, Grob does not and cannot remedy the above-identified deficiencies of the combination of Fehnel, Chakrabarti, and Marcovici, and the combination of Fehnel, Chakrabarti, Marcovici, and Grob fails to disclose or suggest all of the elements of claims 6-9 and 14-18.

Moreover, there is no legally sufficient motivation to combine Grob with Fehnel, Chakrabarti, and Marcovici. The Office Action asserted that the motivation to combine

would be “because it offers the advantage of providing an industry standard protocol for authentication using the RADIUS protocol,” citing Grob at column 2, lines 54-60. This proposal is legally insufficient for several reasons.

The cited passage simply mentions that a RADIUS server is used in Grob. Grob does not indicate that using a RADIUS server in particular produces any advantages. At least some of the other cited references describe using authentication methods that are inconsistent with the RADIUS approach. Thus, the proposed modification is not merely an issue of standardizing an approach but of substituting one approach for another.

Finally, this alleged motivation to combine is simply a motivation to use Grob as-is — not a motivation to combine Grob with the teachings of any of the three other references. Thus, for each of these reasons, a *prima facie* motivation to combine Grob with the other references has not been provided, and there is no teaching, motivation, suggestion, or other reason in Grob that would remedy the motivational deficiencies of the combination of Fehnel, Chakrabarti, and Marcovici as set forth above.

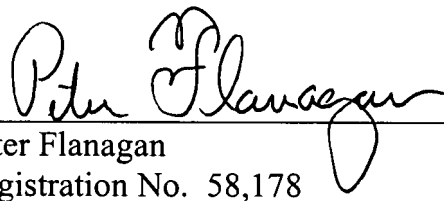
Accordingly, for all these reasons, it is respectfully requested that the rejection of claims 6-9 and 14-18 be withdrawn.

For the reasons set forth above, it is respectfully submitted that each of claims 1-2 and 4-21 recites subject matter that is neither disclosed nor suggested in the cited art. It is, therefore, respectfully requested that all of claims 1-2 and 4-21 be allowed, and that this application be passed to issuance.

If, for any reason, the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, Applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, Applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,


Peter Flanagan
Registration No. 58,178

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800; Fax: 703-720-7802

PCF:jkm:kh

Enclosures: Petition for Extension of Time
Check No. 16590